

**IN THE UNITED STATES DISTRICT COURT FOR THE
EASTERN DISTRICT OF NORTH CAROLINA**

**RICKEY KIMBRIEL and PAULA
KIMBRIEL, on behalf of themselves
and all others similarly situated,**

Plaintiffs,

v.

**ABB INC., and BALDOR
ELECTRIC COMPANY N/K/A ABB
MOTORS AND MECHANICAL
INC.,**

Defendants.

Case No. 5:19-cv-00215

CLASS ACTION COMPLAINT

JURY DEMANDED

CLASS ACTION COMPLAINT

Plaintiffs Rickey and Paula Kimbriel (“Plaintiffs”), individually and on behalf of the class set forth below, bring the following class action complaint against defendants ABB, Inc. (“ABB”) and Baldor Electric Company N/K/A ABB Motors and Mechanical, Inc. (“Baldor”) (collectively, “Defendants”):

PRELIMINARY STATEMENT

1. This case is about a substantial data security breach, affecting nearly 18,000 employees and their family members who are participants in the ABB health benefits plan (the “Plan”).

2. As a result of this breach, Plaintiffs and the class members whose personal information was not safeguarded have suffered identity theft and have been forced to expend substantial time and money to protect themselves from the substantial risk of further injury from identity theft, credit and reputational injury, false tax claims, or even extortion they now face.

3. Prior to August 25, 2017, hackers, utilizing a well-known “phishing” or scam email scheme, compromised Plan accounts containing participants’ personally identifying information (“PII”). This PII included sensitive information such as names, addresses, plan member IDs, birth dates, social security numbers, FMLA information, and direct deposit information.

4. ABB did not publicly acknowledge the data breach or begin notifying the Plan participants until on or after September 7, 2017.

5. According to its Form 5500 filed with the United States Department of Labor, there were approximately 17,996 active participants in the Plan as of the end of 2016. All of those 17,996 Plan participants had their PII compromised by the data breach.

6. The data security breach was caused by ABB’s knowing violation of its obligation to secure its employees’ and their family members’ personal information.

7. ABB failed to comply with security standards and allowed the Plan participants’ PII to be compromised.

8. As a consequence of the data security breach, Plaintiffs and Class Members have suffered damages by taking measures to deter, detect, and stop identity theft. Class Members have been required to take the time, which they otherwise would have dedicated to other life demands (such as work), and effort to mitigate the actual and potential impact of the data breach on their lives including, inter alia; placing “freezes” and “alerts” with credit reporting agencies, contacting their financial institutions, closing or modifying financial accounts, scheduling and attending appointments with the IRS, closely reviewing and monitoring their credit reports and accounts for unauthorized activity, responding to unauthorized activity on their credit reports, contacting the Social Security office, and filing police reports.

9. No one can know what else the cyber criminals will do with the employees' PII. However, what is known is that the purpose of the phishing scheme was to obtain participants' PII. ABB employees and their family members are now, and for the rest of their lives will be, at a heightened risk of further identity theft and fraud. For all Class Members, fear and anxiety of identity theft or fraud is the new norm.

10. Plaintiffs seek redress individually, and on behalf of those similarly situated, for the injuries that they and class members sustained as a result of ABB's negligent and intentional violations of law.

11. Plaintiffs assert these claims on behalf of a nationwide class of participants in the Plan for monetary relief, injunctive relief, corresponding declaratory relief, and other appropriate relief for ABB's unlawful conduct, as described herein.

PARTIES

12. Plaintiffs are Arkansas citizens residing in Franklin County, Arkansas. Plaintiff Rickey Kimbriel works for Baldor Electric Company in Ozark, Arkansas, which, beginning March 1, 2018, changed its name to ABB Motors and Mechanical Inc. He has been a participant in the Plan since at least 2015. Plaintiff Paula Kimbriel is Rickey Kimbriel's spouse, his dependent, and has been a beneficiary covered by the Plan since at least 2015.

13. Defendant ABB, Inc. ("ABB") is an industrial technologies company incorporated in Delaware, with its principal place of business in Cary, North Carolina. ABB may be served with process upon its registered agent C T Corporation System, 160 Mine Lake Court, Suite 200, Raleigh, North Carolina.

14. Defendant Baldor Electric Company n/k/a ABB Motors and Mechanical Inc. ("Baldor") is a Missouri corporation, with its principal place of business in Fort Smith, Arkansas.

ABB Motors and Mechanical Inc. may be served with process upon its registered agent CT Corporation System, 120 South Central Avenue, Clayton, MO 63105.

15. Collectively, ABB and Baldor will be referred to herein as “ABB” or “Defendants.”

16. Upon information and belief, ABB’s wrongful acts and omissions leading to this data security breach occurred nationwide and in this district.

JURISDICTION AND VENUE

17. This Court has subject matter jurisdiction over this action under the Class Action Fairness Act, 28 U.S.C. § 1332(d)(2). The amount in controversy exceeds \$5 million exclusive of interest and costs. Plaintiff, the class members, and ABB are citizens of different states. There are more than 100 putative class members.

18. This court has personal jurisdiction over ABB because Plaintiffs’ claims arise out of ABB’s contacts with North Carolina.

19. Venue is proper in this court pursuant to 28 U.S.C. § 1391(b), (c), and (d). ABB is registered to do business, transacted business, were founded in, and had agents in this district; a substantial part of the events giving rise to the Plaintiffs’ claims arose in this district, and a substantial portion of the affected interstate commerce described below has been carried out in this district.

ALLEGATIONS OF FACT

20. Plaintiff Rickey Kimbriel has worked as a machine operator at Baldor’s facility in Ozark, Arkansas since 2015.

21. At all relevant times, Baldor was a subsidiary of ABB.

22. Baldor's employee handbook received by Plaintiff makes the following pledges to its employees:

- a) The Company's code of ethics is "I will not lie, cheat, steal, nor tolerate those who do."
- b) The Company "work[s] hard every day to be the safest place to work."
- c) The Company "will attempt to keep you fully informed about matters that affect you" and "will be honest in [its] communications and dealings with you"
- d) The Company "will do what is right."
- e) The Company believes [i]t is important to have current and correct information about you. We need the information for Social Security, withholding taxes, insurance, and emergencies."

23. Plaintiff Rickey Kimbriel was a participant in the Plan at all relevant times. The Plan includes health care coverage, short term disability, long term disability, life insurance, and 401(k).

24. Plaintiff Rickey Kimbriel gave ABB information with respect to his checking account at the Bank of the Ozarks for the purpose of direct deposit of his paycheck.

25. When Plaintiff Rickey Kimbriel enrolled in the Plan, he provided sensitive personal information about himself and his dependent Paula Kimbriel, including full legal names, addresses, birth dates, and social security numbers.

26. Upon information and belief, this information was entered into the Plan's database under Plaintiff Rickey Kimbriel's account, which ABB and Baldor stored and maintained in electronic form along with other information pertinent to Plaintiff Rickey Kimbriel's employee benefits, such as plan member ID.

27. Upon information and belief, the same sensitive personal information regarding Plaintiff Rickey Kimbriel's account maintained and accessible in the Plan's database was maintained and/or accessible through certain ABB employee email accounts.

28. The Company called a meeting near the end of August, 2017 to inform Plaintiff Rickey Kimbriel and other employees on his shift that there had been a breach of their data, and that they would follow up with more information in the near future. In that same meeting, the Company informed the employees it would provide at least one year of credit monitoring.

29. Nearly two weeks later in September 2017, Plaintiff Rickey Kimbriel received a letter from the Head of Human Resources at ABB, Dorothea Klein, to his home address dated September 7, 2017 titled "**Notice of Data Breach.**" (Attached as **Exhibit A**). The letter stated that Plaintiff Rickey Kimbriel and his dependents' sensitive personally identifying information ("PII") associated with the Plan's benefits may have been exposed as a result of a phishing scheme on ABB employee email accounts. The letter identified that the compromised accounts may have specifically exposed names, addresses, plan member IDs, birth dates, and social security numbers. The letter also represented that before notifying Plaintiff Rickey Kimbriel, ABB had already conducted a "full assessment to determine the scope of the data exposed and identify any potentially affected individuals."

30. According to the Federal Trade Commission ("FTC"), "phishing" is when a scammer uses fraudulent emails or texts, or copycat websites to get someone to share valuable personal information, "such as account numbers, social security numbers, or your login IDs and passwords," and then uses this information to steal money or identity or both.¹ By acknowledging that Plaintiff Rickey Kimbriel's personal information was exposed as the result of a "phishing scheme," ABB has acknowledged that the data thief intentionally targeted

¹ <https://www.consumer.ftc.gov/articles/how-recognize-and-avoid-phishing-scams>

Plaintiff Rickey Kimbriel and class members' personal information which was compromised in the ABB data breach.

31. The FTC defines identity theft as “a fraud committed or attempted using the identifying information of another person without authority.”² The FTC describes “identifying information” as “any name or number that may be used, alone or in conjunction with any other information, to identify a specific person,” including, among other things, “[n]ame, Social Security number, date of birth, official State or government issued driver’s license or identification number, alien registration number, government passport number, employer or taxpayer identification number.”³

32. Social Security numbers, for example, are among the worst kind of personal information to have stolen because they may be put to a variety of fraudulent uses and are difficult for an individual to change.

33. The Social Security Administration has warned that identity thieves can use an individual’s Social Security number to apply for additional credit lines. Such fraud may go undetected until debt collection calls commence months, or even years, later.⁴

34. Stolen Social Security numbers also make it possible for thieves to file fraudulent tax returns, file for unemployment benefits, or apply for a job using a false identity. Each of these fraudulent activities is difficult to detect. An individual may not know that his or her Social Security number was used to file for unemployment benefits until law enforcement notifies the individual’s employer of the suspected fraud. Fraudulent tax returns are typically discovered only when an individual’s authentic tax return is rejected. What is more, it is no easy task to

² 17 C.F.R. § 248.201 (2013).

³ *Id.*

⁴ Social Security Administration, Identity Theft and Your Social Security Number, *available at* <http://www.ssa.gov/pubs/EN-05-10064.pdf> (last visited May 20, 2019).

change or cancel a stolen Social Security number. An individual cannot obtain a new Social Security number without significant paperwork and evidence of actual misuse. In other words, preventive action to defend against the possibility of misuse of a Social Security Number is not permitted; an individual must show evidence of actual, ongoing fraud activity to obtain a new number.

35. Even then, a new Social Security number may not be effective. According to Julie Ferguson of the Identity Theft Resource Center: “The credit bureaus and banks are able to link the new number very quickly to the old number, so all of that old bad information is quickly inherited into the new Social Security number.”⁵

36. Based on the foregoing, the information stolen in the data breach is significantly more valuable than the loss of, say, credit card information in a large retailer data breach such as those that occurred at Target and Home Depot. Victims affected by those retailer breaches could avoid much of the potential future harm by cancelling credit or debit cards and obtaining replacements. The information stolen in the data breach is difficult, if not impossible, to change—Social Security number, name, employment information, income data, etc.

37. This data, as one would expect, demands a much higher price on the black market. Martin Walter, senior director at cybersecurity firm RedSeal, explained, “Compared to credit card information, personally identifiable information and Social Security numbers are worth more than 10x on the black market.”⁶

⁵ *Victims of Social Security Number Theft Find It's Hard to Bounce Back*, NPR, Brian Naylor, Feb. 9, 2015, available at <http://www.npr.org/2015/02/09/384875839/data-stolen-by-anthem-s-hackershas-millions-worrying-about-identity-theft> (last visited May 20, 2019).

⁶ *Anthem Hack: Personal Data Stolen Sells for 10x Price of Stolen Credit Card Numbers*, IT World, Tim Greene, Feb. 6, 2015, available at <https://www.networkworld.com/article/2880366/anthem-hack-personal-data-stolen-sells-for-10x-price-of-stolen-credit-card-numbers.html> (last visited May 20, 2019).

38. Among other forms of fraud, identity thieves may obtain driver's licenses, government benefits, medical services, and housing or even give false information to police during an arrest.

39. The fraudulent activity resulting from the data breach may not come to light for years.

40. In the "Notice of Data Breach," ABB also represented that it would pay for Plaintiff and Class Members to have one (1) year of identity monitoring services provided by risk mitigation and response entity Kroll. The letter further advised Plaintiff as to additional steps he should take to protect himself, including placing a fraud alert with the Federal Trade Commission and placing a security freeze on his credit file. However, the letter said nothing about offering any relief like identity theft monitoring services to Plaintiff Paula Kimbriel or other similarly affected dependents.

41. In November 2017, specifically in response to the breach for fear that his information would be further compromised, Plaintiff Rickey Kimbriel stopped making his two percent (2%) deferrals to his 401(k). But for the data breach, Plaintiff Rickey Kimbriel would have made those deferrals. As a consequence, he was taxed on income that he otherwise would have invested tax-deferred, and therefore has suffered and will continue to suffer actual economic loss as a consequence.

42. Plaintiffs' fear of identity theft resulting from their compromised information has already proven well grounded. Plaintiff Paula Kimbriel was notified by a credit-monitoring service that on February 13, 2019, there were five unauthorized credit inquiries with banking institutions in four different states, indicating identity theft. In response, Plaintiffs have spent

significant time to begin the process to dispute the identity theft. This has only increased Plaintiffs' fears and time spent as a result of the data breach.

43. ABB has failed to provide compensation to Plaintiffs and Class Members victimized in this data breach. ABB has not offered to provide any assistance or compensation for the costs and burdens – current and future – associated with the identity theft and fraud resulting from the data breach. ABB has not offered Plaintiffs or Class Members any assistance in dealing with the IRS or state tax agencies.

44. It is incorrect to assume that reimbursing a consumer for financial loss due to fraud makes that individual whole again. On the contrary, after conducting a study, the U.S. Department of Justice's Bureau of Justice Statistics found that "among victims who had personal information used for fraudulent purposes, 29% spent a month or more resolving problems" and that "resolving the problems caused by identity theft [could] take more than a year for some victims."⁷

45. As a result of ABB's failure to prevent the data breach, Plaintiffs Rickey and Paula Kimbriel and Class Members have suffered and will continue to suffer damages, including monetary losses, lost time, anxiety and emotional distress. They have suffered or are at increased risk of suffering:

- a. The loss of the opportunity to control how their PII is used;
- b. The diminution in value of their PII;
- c. The compromise, publication and/or theft of their PII;
- d. Out-of-pocket costs associated with the prevention, detection, recovery and remediation from identity theft or fraud;

⁷ Victims of Identity Theft, 2012 (Dec. 2013) at 10, 11, *available at* <https://www.bjs.gov/content/pub/pdf/vit12.pdf> (last visited May 20, 2019).

- e. Lost opportunity costs and lost wages associated with effort expended and the loss of productivity from addressing and attempting to mitigate the actual and future consequences of the data breach, including but not limited to efforts spent researching how to prevent, detect, contest and recover from identity theft and fraud;
- f. Delay in receipt of tax refund monies;
- g. Unauthorized use of stolen PII;
- h. The continued risk to their PII, which remains in the possession of ABB and is subject to further breaches so long as ABB fail to undertake appropriate measures to protect the PII in their possession; and
- i. Current and future costs in terms of time, effort and money that will be expended to prevent, detect, contest, remediate and repair the impact of the data breach for the remainder of the lives of Plaintiff and Class Members.

CLASS ACTION ALLEGATIONS

46. Plaintiffs and the class members, as defined below, have been damaged by ABB's negligent or reckless disregard for their personal information, as well as ABB's intentional silence regarding the existence and nature of the data security breach.

47. Plaintiffs bring this action as a class action pursuant to Rule 23 of the Federal Rules of Civil Procedure.

48. Plaintiffs assert the claims herein on behalf of a proposed Nationwide Class ("the Class") defined as follows:

All United States residents whose information was made accessible to an unauthorized third party in the data security breach announced by ABB on September 7, 2017.⁸

⁸ The following are excluded from the Nationwide Class: (1) the defendants, their parent companies, subsidiaries and affiliates, and any co-conspirators; and (2) any judge or magistrate presiding over this action, and members of their families. The Plaintiffs reserve the right to amend the class period and/or class definition if discovery and further investigation reveal that

49. **Numerosity.** The members of the class are so numerous that joinder of all class members is impracticable. Nearly 18,000 Plan participants are affected by the data security breach.

50. **Typicality.** Plaintiffs' claims are typical of other class members because, among other things, all class members' PII was exposed to an unauthorized third party by ABB's negligent, reckless, and intentional conduct, as described above, which caused the data security breach.

51. **Adequacy.** Plaintiffs will fairly and adequately protect the interests of the class. Furthermore, they have retained counsel experienced in class actions and complex litigation.

52. **Commonality and Predominance.** Common questions of law and fact exist as to all class members and predominate over any questions solely affecting individual members of the class, including but not limited to:

a) whether ABB owed duties under federal or state law to class members to protect their personal information, provide timely notice of unauthorized access to this information, and provide meaningful and fair redress;

b) whether ABB breached said duties;

c) whether ABB acted wrongfully by improperly monitoring, storing, and/or failing to properly safeguard the class members' personal information;

d) whether ABB knew, or reasonably should have known, about the deficiencies in its data security protocols;

e) whether ABB willfully failed to design, employ, and maintain adequate security safeguards to protect employees' personal information;

the class should be expanded, divided into additional subclasses, or modified in any way.

- f) whether ABB's representations regarding the security of its systems were false and misleading;
- g) whether ABB's acts and omissions violated applicable state consumer protection law;
- h) whether ABB's failures resulted in the data security breach at issue;
- i) whether ABB failed to properly and timely notify Plaintiffs and class members of the breach as soon as practicable after it was discovered;
- j) whether ABB's acts of concealment violated applicable state consumer protection laws; and
- k) whether class members have been damaged and, if so, the appropriate relief.

53. **Superiority.** Consistent with Rule 23(b)(3), a class action is superior to any other available means for the fair and efficient adjudication of this controversy, and no unusual difficulties are likely to be encountered in the management of this class action. The present litigation involves a textbook example of the superior quality of a class action mechanism to resolve millions of claims in a single litigation that may otherwise be uneconomical to pursue in individual litigation. The burden and expense of litigating the present case in an individual capacity is comparatively high compared to the individual recovery of any individual Plaintiff or putative class member. Without the Rule 23 class mechanism, Plaintiffs and the Class would be without a practical path to remedy defendants' wrongful conduct.

54. This case is maintainable as a class action under Fed. R. Civ. P. 23(b)(2) because the defendants have acted or refused to act on grounds that apply generally to the class, so that final injunctive relief or corresponding declaratory relief is appropriate respecting the class as a whole.

55. Class certification is also appropriate under Fed. R. Civ. P. 23(b)(3) because questions of law and fact common to the class predominate over any questions affecting only individual members of the class, and because a class action is superior to other available methods for the fair and efficient adjudication of this controversy.

56. ABB's conduct as described in this complaint stems from common and uniform policies and practices, resulting in a colossal data security breach as well as a deliberate and systematic cover-up scheme to hide the extent and nature of the breach from regulators as well as those affected by the breach.

57. The class members do not have an interest in pursuing separate individual actions against ABB, as the amount of each class member's individual claims are small compared to the expense and burden of individual prosecution.

58. Class certification also will obviate the need for unduly duplicative litigation that might result in inconsistent judgments concerning ABB's practices. Moreover, management of this action as a class action will not present any likely difficulties. In the interests of justice and judicial efficiency, it would be desirable to concentrate the litigation of all class members' claims in a single forum.

59. Plaintiffs intend to send notice to all class members to the extent required by Rule 23.

CLAIMS FOR RELIEF

COUNT I – VIOLATION OF NORTH CAROLINA UNFAIR OR FRAUDULENT BUSINESS PRACTICES (On behalf of the Nationwide Class)

60. Plaintiffs, on behalf of the Nationwide Class, allege and incorporate by reference the allegations in the preceding paragraphs.

61. ABB, as a North Carolina based entity, is subject to the laws and regulations of the State of North Carolina, including but not limited to the North Carolina Unfair & Deceptive Trade Practices Act, N.C. Gen. Stat. § 75-1.1 (“North Carolina UDTPA”). The North Carolina UDTPA “declare[s] unlawful” all “[u]nfair methods of competition in or affecting commerce, and unfair or deceptive acts or practices in or affecting commerce.” *Id.* § 75-1.1(a).

62. For purposes of North Carolina UDTPA, the term “‘commerce’ includes all business activities, however denominated, but does not include professional services rendered by a member of a learned profession.” *Id.* § 75-1.1(b).

63. ABB violated the North Carolina UDTPA by engaging in unlawful, unfair, or deceptive business acts and practices in or affecting commerce, as well as unfair, deceptive, untrue, or misleading advertising that constitute acts of “unfair competition” prohibited in the North Carolina UDTPA.

64. ABB engaged in unlawful acts and practices with respect to their services by establishing inadequate security practices and procedures described herein; by soliciting and collecting Plaintiffs’ and class members’ personal information with knowledge that such information would not be adequately protected; and by gathering Plaintiffs’ and class members’ personal information in an unsecure electronic environment in violation of North Carolina’s data breach statute, the Identity Theft Protection Act, N.C. Gen. Stat. § 75-60, *et seq.*, which requires ABB to undertake reasonable methods of safeguarding the personal information of Plaintiffs Rickey Kimbriel, Paula Kimbriel and the class members.

65. In addition, ABB engaged in unlawful acts and practices when it failed to discover and then disclose the data security breach to Plaintiffs and the class members in a timely and accurate manner, contrary to the duties imposed by N.C. Gen. Stat. § 75-65.

66. To date, ABB still has not provided sufficient information regarding the data security breach to Plaintiffs and the class members.

67. As a direct and proximate result of ABB's unlawful acts and practices, Plaintiffs and the class members were injured and lost money or property, including but not limited to the loss of their legally protected interests in the confidentiality and privacy of their personal information.

68. ABB knew or should have known that their data security practices were inadequate to safeguard Plaintiffs and the class members' personal information, that the risk of a data security breach was significant, and that their system was, in fact, breached.

69. ABB's actions in engaging in the above-named unlawful practices were negligent, knowing and willful, and/or wanton and reckless with respect to the rights of Plaintiffs and the class members.

70. Plaintiffs and the class members seek relief under the North Carolina UDTPA including, but not limited to: restitution to Plaintiffs and class members of money and property that ABB has acquired by means of unlawful and unfair business practices; disgorgement of all profits accruing to ABB because of its unlawful and unfair business practices; treble damages (pursuant to N.C. Gen. Stat. § 75-16); declaratory relief; attorneys' fees and costs (pursuant to N.C. Gen. Stat. § 75-16.1); and injunctive or other equitable relief.

COUNT II – BREACH OF FIDUCIARY DUTIES
(On behalf of the Nationwide Class)

71. Plaintiffs, on behalf of the nationwide class, allege and incorporate by reference the allegations in the preceding paragraphs.

72. ABB, by virtue of its possession, custody, and/or control of Plaintiffs and the class members' personal information, and ABB's duty to properly monitor and safeguard said

information, was, and continues to be, in a confidential, special, and/or fiduciary relationship with Plaintiffs and the class members.

73. As a fiduciary, ABB owed, and continues to owe, Plaintiffs and the class members:

- (a) the commitment to deal fairly and honestly;
- (b) the duties of good faith and undivided loyalty; and
- (c) integrity of the strictest kind.

74. ABB was, and continues to be, obligated to exercise the highest degree of care in carrying out the responsibilities to Plaintiffs and class members under such confidential, special, and/or fiduciary relationships.

75. ABB breached its fiduciary duties to Plaintiffs and the class members when it failed to adequately store, monitor, and protect Plaintiff Rickey and Paula Kimbriel's and class members' personal information.

76. ABB willfully and wantonly breached its fiduciary duties to Plaintiffs and the class members or, at the very least, committed these breaches with conscious indifference and reckless disregard of Plaintiffs and the class members' rights and interests.

COUNT III – NEGLIGENCE
(On behalf of Nationwide Class)

77. Plaintiffs, on behalf of the Nationwide Class, allege and incorporate by reference the allegations in the preceding paragraphs.

78. ABB was, and continues to be, in a confidential, special, and/or fiduciary relationship with Plaintiffs and the class members by virtue of being trusted with their personal information.

79. Upon accepting and storing the personal information of Plaintiffs and the class

members in its computer systems and on its networks, ABB undertook and owed a duty to Plaintiffs and the class members to exercise reasonable care to secure and safeguard that information and to use commercially reasonable methods to do so. ABB knew that the personal information was private and confidential and should be protected as such.

80. At the very least, ABB assumed a duty, and had duties imposed upon it by regulations, to comply with applicable security standards, regulations, and statutes, and to otherwise use reasonable care to safeguard Plaintiffs and the class members' personal information. ABB owed a duty of care to Plaintiffs and the class members to safeguard their personal information because Plaintiffs and the class members were foreseeable and probable victims of any cyberattack that successfully stole or obtained personal information stored within ABB's data security systems.

81. ABB knew, or should have known, of the risks inherent in collecting and storing personal information, the vulnerabilities of its data security systems, and the importance of adequate security. ABB knew, or should have known, that its data systems and networks did not adequately safeguard the personal information of Plaintiffs and the class members.

82. ABB's own conduct also created a foreseeable risk of harm to Plaintiffs and the class members and their personal information. Upon information and belief, ABB's misconduct included failing to: (1) secure its systems, despite knowing their vulnerabilities; (2) comply with industry standard security practices; (3) implement adequate system and event monitoring; and (4) implement the systems, policies, and procedures necessary to prevent this type of data breach.

83. Through ABB's acts and omissions described herein, including ABB's failure to provide adequate security and its failure to protect the personal information of Plaintiffs and the

class members from being foreseeably accessed, captured, stolen, disseminated, and misused, ABB unlawfully breached its duty to use reasonable care to adequately protect and secure the personal information of Plaintiffs and the class members during the time it was in ABB's possession or control.

84. ABB also had a duty to timely inform Plaintiffs and the class members of the data security breach, and of the fact that their personal information had been compromised and/or stolen; furthermore, upon learning of the breach, ABB had a duty to take immediate action to protect Plaintiffs and the class members from the foreseeable consequences of the breach.

85. By its acts and omissions as described herein, ABB unlawfully breached its duty and Plaintiffs and the class members were harmed as a direct result.

86. ABB knew, or should have known, that its system for processing and storing class members' personal information was replete with security vulnerabilities.

87. ABB was negligent by continuing to accept, process, and store such information in light of its computer system vulnerabilities and the sensitivity of the personal information stored therein.

88. The data security breach, and resulting damages suffered by Plaintiffs and the class members, were the direct and proximate result of a number of actions and omissions, including but not limited to:

- (a) ABB's improper retention and storage of Plaintiffs and class members' personal information;
- (b) ABB's failure to use reasonable care to implement and maintain appropriate security procedures reasonably designed to protect such information;
- (c) ABB's delay before notifying Plaintiff Rickey Kimbriel and class members about

the breach; and

(d) ABB's failure to take immediate and effective action to protect Plaintiffs and class members from potential and foreseeable damage.

89. ABB's wrongful actions, as described above, reflect a breach of the duty of reasonable care and, therefore, constitute negligence.

90. Plaintiffs and the class members have not in any way contributed to the data security breach or theft of their personal information.

COUNT IV – NEGLIGENCE PER SE
(On behalf of the Nationwide Class)

91. Plaintiffs, on behalf of the Nationwide Class, allege and incorporate by reference the allegations in the preceding paragraphs.

92. Section 5 of the FTC Act prohibits “unfair . . . practices in or affecting commerce,” including, as interpreted and enforced by the FTC, the unfair act or practice by businesses, such as ABB, of failing to use reasonable measures to protect personal information. The FTC has pursued numerous enforcement actions under Section 5 of the FTC Act against businesses, which, as a result of their failure to employ reasonable data security measures and avoid unfair and deceptive practices, caused the same harm as that suffered by Plaintiffs and class members.

93. ABB violated Section 5 of the FTC Act by failing to use reasonable measures to protect the personal information of Plaintiffs and the class members and not complying with applicable industry standards, as described in detail herein. ABB's conduct was particularly unreasonable given the nature and amount of personal information it obtained and stored, and the foreseeable consequences of a data breach at a corporation such as ABB, including, specifically, the immense damages that would result to Plaintiffs and the class members.

94. ABB's violation of Section 5 of the FTC Act constitutes negligence per se.

95. Plaintiffs and the class members are within the class of persons that the FTC Act was intended to protect.

96. The harm that occurred as a result of the data breach is the type of harm the FTC Act was intended to guard against.

97. As a direct and proximate result of ABB's negligence per se, Plaintiffs and class members have suffered, and continue to suffer, injuries and damages arising from the data breach as described herein.

COUNT VI – BAILMENT
(On behalf of the Nationwide Class)

98. Plaintiffs, on behalf of the Nationwide Class, allege and incorporate by reference the allegations in the preceding paragraphs.

99. Plaintiffs and the class members' personal information is their property, which they delivered to ABB for the sole and specifying purpose of completing one or more commercial transactions.

100. ABB accepted Plaintiff Rickey Kimbriel, Paula Kimbriel and class members' personal information and, thus, served as a bailee with respect to the above-referenced transaction(s).

101. ABB, as a bailee, owed a duty to Plaintiffs and class members and, in fact, had an express and/or implied contract with them to protect their personal information from theft, compromise, or unauthorized disclosure.

102. ABB breached its duty and/or express and implied contracts with Plaintiffs and class members by improperly storing and inadequately protecting their personal information from theft, compromise, and/or unauthorized disclosure, which directly and proximately caused

Plaintiff and class members to suffer damages.

103. ABB's wrongful actions constitute breaches of their duty (and/or express and/or implied contracts) with Plaintiffs and the class members arising from the bailment.

COUNT VII– BREACH OF CONTRACT
(On behalf of the Nationwide Class)

104. Plaintiffs incorporate by reference those paragraphs set out above as if fully set forth herein.

105. ABB has a contractual obligation to maintain the security of its employees and their family members' PII, which ABB itself recognizes in its handbook.

106. ABB breached that contractual obligation by failing to safeguard and protect the PII of Plaintiffs and members of the Class and by failing to provide timely and accurate notice to them that their PII was compromised in and as a result of the ABB data breach.

107. The losses and damages sustained by Plaintiffs and Class members as described herein were the direct and proximate result of ABB's breaches of the contracts between ABB and Plaintiffs and members of the Class.

COUNT VIII – BREACH OF IMPLIED CONTRACT
(On behalf of the Nationwide Class)

108. Plaintiffs, on behalf of the Nationwide Class, allege and incorporate by reference the allegations in the preceding paragraphs.

109. Plaintiffs and Class members were required to provide their PII, including names, addresses, Social Security numbers, and other personal information, to ABB as a condition of their employment.

110. Implicit in the employment agreement between ABB and its employees was the

obligation that both parties would maintain information confidentially and securely.

111. ABB had an implied duty of good faith to ensure that the PII of Plaintiffs and Class members in its possession was only used to provide the Plan and other employment benefits from ABB.

112. ABB had an implied duty to reasonably safeguard and protect the PII of Plaintiffs and Class members from unauthorized disclosure or uses.

113. Additionally, ABB implicitly promised to retain this PII only under conditions that kept such information secure and confidential.

114. Plaintiffs and Class members fully performed their obligations under the implied contract with ABB. ABB did not.

115. Plaintiffs and Class members would not have provided their confidential PII to ABB in the absence of their implied contracts with ABB, and would have instead retained the opportunity to control their PII for uses other than the Plan and employment benefits from ABB.

116. ABB breached the implied contracts with Plaintiffs and Class members by failing to reasonably safeguard and protect Plaintiffs' and Class members' PII, which was compromised as a result of the data breach.

117. ABB's acts and omissions have materially affected the intended purpose of the implied contracts requiring Plaintiffs and Class members to provide their PII as a condition of employment in exchange for the Plan, compensation and benefits.

118. As a direct and proximate result of ABB's breach of its implied contracts with Plaintiffs and Class members, Plaintiffs and Class members have suffered and will suffer injury, including but not limited to: (i) the loss of the opportunity how their PII is used; (ii) the

compromise, publication, and/or theft of their PII; (iii) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, tax fraud, and/or unauthorized use of their PII; (iv) lost opportunity costs associated with effort expended and the loss of productivity addressing and attempting to mitigate the actual and future consequences of the data breach, including but not limited to efforts spent researching how to prevent, detect, contest and recover from tax fraud and identity theft; (v) costs associated with placing freezes on credit reports; (vi) the continued risk to their PII, which remain in ABB's possession and is subject to further unauthorized disclosures so long as ABB fails to undertake appropriate and adequate measures to protect the PII of employees and former employees in its continued possession; and, (vii) future costs in terms of time, effort and money that will be expended to prevent, detect, contest, and repair the impact of the PII compromised as a result of the data breach for the remainder of the lives of Plaintiffs and Class members.

PRAYER FOR RELIEF

As a direct and proximate cause of ABB's wrongful conduct, Plaintiffs and the class members sustained, and will continue to incur, damages in the form of:

- a) the unauthorized disclosure and/or compromise of their personal information;
- b) monetary losses and damage to credit from fraudulent charges made upon their accounts; and
- c) the burden and expense of credit monitoring.

Accordingly, Plaintiffs, individually and on behalf of the class, requests relief as follows:

- a) certification of the Nationwide Class pursuant to Fed. R. Civ. P. 23, as requested herein;
- b) appointment of Plaintiffs Rickey and Paula Kimbriel as class representatives, and the undersigned counsel as class counsel;
- c) an order directing that reasonable notice of this action, as provided by Fed. R. Civ. P. 23(c)(2), be given to each and every class member;

d) equitable relief to prevent any additional harm including, but not limited to, provision of credit monitoring services for a period of time to be determined by a trier of fact;

e) an injunction permanently enjoining ABB, as well as its subsidiaries and affiliates from further engaging in the same acts or omissions that led to the data security breach described above;

f) a judgment in favor of Plaintiffs and class members under the legal theories alleged herein;

g) an award to the Plaintiffs and class members of nominal damages, compensatory damages, and/or punitive damages, to the extent allowed by law;

h) an award to the Plaintiffs and class members of restitution and/or disgorgement of profits;

i) an award of pre- and post-judgment interest as provided by law, and that such interest be awarded at the highest legal rate from and after the date of service of this complaint;

j) an award of reasonable attorneys' fees, costs, and expenses; and

k) granting such other relief as the court deems just and proper.

DEMAND FOR JURY TRIAL

Pursuant to Rule 38(b) of the Federal Rules of Civil Procedure, the Plaintiffs and the class demand a trial by jury.

Dated: May 22, 2019

Respectfully submitted,

/s/ Narendra K. Ghosh

Narendra K. Ghosh, NC Bar No. 37649

PATTERSON HARKAVY LLP

100 Europa Dr., Suite 420

Chapel Hill, NC 27517

(919) 942-5200

nghosh@pathlaw.com

/s/ Joe P. Leniski Jr.

JOE P. LENISKI, JR. (TN BPR#22891)
(*pro hac vice* application forthcoming)

**BRANSTETTER STRANCH &
JENNINGS, PLLC**

The Freedom Center
223 Rosa L. Parks Ave., Suite 200
Nashville, Tennessee 37203
(615) 254-8801
joeyl@bsjfirm.com

James A. Streett (Ark. Bar No. 2007092)
(*pro hac vice* application forthcoming)

STREETT LAW FIRM, P.A.

107 West Main
Russellville, AR 72801
(479) 968-2030
Alex@StreettLaw.com
James@StreettLaw.com

Lynn A. Toops (Ind. Bar No. 26386-49)
(*pro hac vice* application forthcoming)

COHEN & MALAD, LLP

One Indiana Square, Suite 1400
Indianapolis, Indiana 46204
(317) 636-6481
ltoops@cohenandmalad.com

ATTORNEYS FOR PLAINTIFFS